

Brief Explanation of the Japanese Publication No. 4-216158

Date of Publication: August 6, 1992

Application No.: 3-36668

Date of Filing: February 7, 1991

Foreign Application Priority Data: February 15, 1990 – USA ... 480437
(USP 5,263,157)

Title of the Invention: Method and system for providing user access control
within a distributed data processing system by the
exchange of access control profiles

Inventor: Frederick L. Janis, Texas, U.S.A.

Applicant: International Business Machines Corporation (U.S.A.)

A method is disclosed for providing user access control for a plurality of resource objects within a distributed data processing system having a plurality of resource managers. A reference monitor service is established and a plurality of access control profiles are stored therein. Thereafter, selected access control profiles are exchanged between the reference monitor service and a resource manager in response to an attempted access of a particular resource object controlled by that resource manager. The resource manager may then control access to the resource object by utilizing the exchanged access control profile. In a preferred embodiment of the present invention, each access control profile may include access control information relating to a selected user; a selected resource object; a selected group of users; a selected set of resource objects; or, a predetermined set of resource objects and a selected group of users.

This Page Blank (uspto)

特開平4-216158

(43) 公開日 平成4年(1992)8月6日

(51) Int.Cl.⁵G 0 6 F 15/16
13/00

識別記号

3 8 0 D 9190-5L
3 5 7 Z 7368-5B

庁内整理番号

F I

技術表示箇所

審査請求 有 請求項の数12(全 8 頁)

(21) 出願番号 特願平3-36668

(22) 出願日 平成3年(1991)2月7日

(31) 優先権主張番号 480437

(32) 優先日 1990年2月15日

(33) 優先権主張国 米国 (US)

(71) 出願人 390009531

インターナショナル・ビジネス・マシー
ズ・コーポレーションINTERNATIONAL BUSIN
ESS MACHINES CORPO
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(72) 発明者 フレデリック・エル・ジャニス

アメリカ合衆国76278、テキサス州、ケラ

ー、クウエイル・ラン 812番地

(74) 代理人 弁理士 碩宮 孝一 (外4名)

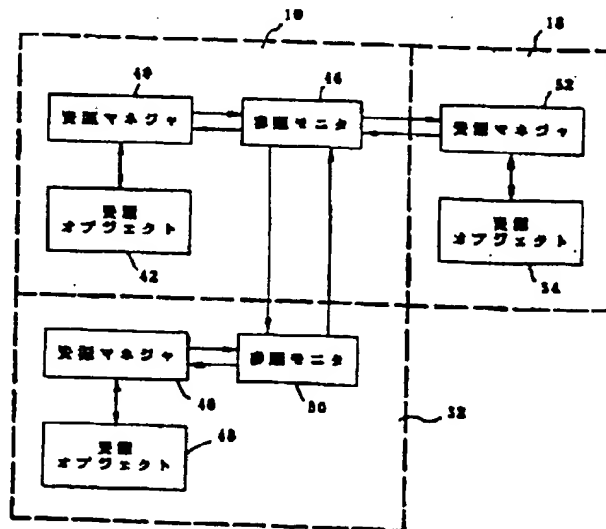
(54) 【発明の名称】 分散データ処理システム内でユーザ・アクセスの制御を実現する方法

(57) 【要約】

【目的】複数の資源マネージャを有する分散データ処理システム内で複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法を提供する。

【構成】参照モニタ・サービス(44、50)を確立し、複数のアクセス制御プロファイルをそこに記憶する。その後、ある資源マネージャ(40、46、52)によって制御される特定の資源オブジェクト(42、48、54)へのアクセスの試みに応答して、選択されたアクセス制御プロファイルが、参照モニタ・サービスとその資源マネージャの間で交換される。その後、資源マネージャは、交換されたアクセス制御プロファイルを用いて、その資源オブジェクトに対するアクセスを制御する。

【効果】分散データ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が実現される。



【特許請求の範囲】

【請求項1】複数の資源オブジェクトに関連づけられた複数の資源マネージャを有する分散データ処理システム内で前記複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法であって、参照モニタ・サービス内に、複数のアクセス制御プロファイルを記憶するステップと、特定の資源オブジェクトへのアクセスの試みに応答して、前記参照モニタ・サービスと選択された資源マネージャの間で、選択されたアクセス制御プロファイルを交換するステップと、前記資源マネージャを利用して、前記選択されたアクセス制御プロファイルに従って、前記特定の資源オブジェクトに対するアクセスを制御するステップとを含む、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項2】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項3】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された資源オブジェクトに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項4】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザ・グループに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項5】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された1組の資源オブジェクトに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項6】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ所定の1組の資源オブジェクトと、それぞれが前記所定の2組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストとに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項7】複数の資源オブジェクトに関連づけられた複数の資源マネージャを有する分散データ処理システム内で前記複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法であって、前記分散データ処理システム内で参照モニタ・サービスを確立するステップと、前記参照モニタ・サービス内に、複数のアクセス制御プロファイルを記憶するステップと、特定の資源オブジェクトへのアクセスの試みに応答して、前記参照モニタ・サービスと選択された資源マネージャの間で、選択さ

れたアクセス制御プロファイルを交換するステップと、前記資源マネージャを利用して、前記選択されたアクセス制御プロファイルに従って、前記特定の資源オブジェクトに対するアクセスを制御するステップとを含む、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項8】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項9】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された資源オブジェクトに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項10】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザ・グループに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項11】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された1組の資源オブジェクトに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項12】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ所定の1組の資源オブジェクトと、それぞれが前記所定の1組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストとに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一般にデータ処理システムに関するものであり、具体的には、分散データ処理システム内の複数の資源オブジェクトに対するアクセスの制御を実現する、改良された方法に関するものである。さらに具体的にいうと、本発明は、分散データ処理システム全体を通じて、アクセス制御情報の高速かつ効率的な交換を可能にするシステムに関するものである。

【0002】

【従来の技術】コンピュータに基づくデータ処理システムにおける、セキュリティおよびアクセス制御システムは、当技術分野で公知である。既存のアクセス制御システムは、一般に、単一ホスト・システム本位のものである。前述の単一ホスト・アクセス制御システムは、ホストのセキュリティと、ファイルなどのシステム資源およびアプリケーションに対するアクセス制御とを実現する

ために利用される。それぞれのアプリケーションは、一般に、そのアプリケーションによって制御される資源に対するアクセス制御を実現しなければならない。

【0003】IBM370システムと共に使用するように設計されたアクセス制御システムの1例が、RACF（資源アクセス管理機能）と称する製品である。RACFは、ファイルやCICS（顧客情報管理システム）トランザクションなど、アプリケーションに対するアクセス制御を提供し、ユーザのアクセス権限レベルおよびグループ化に関して階層本位になっている。RACFは、「パスワード」本位のアクセス制御システムであり、ユーザ個人の識別と、その識別を検証するのに適したパスワードをユーザが知っているかどうかに基づいて、アクセスが許可または拒否される。しかし、RACFは、単一ホストシステム本位のものであり、別々の資源オブジェクトのグループに関連づけられた複数のホストを使用する、分散データ処理システムでは使用できない。というのは、このシステムでは、あるホストから別のホストへのアクセス制御情報の交換が可能でないからである。

【0004】既知のアクセス制御システムのもう1つの例が、AS/400である。AS/400システムは、ケイパビリティ（資格）に基づくシステムであり、セキュリティは、それぞれの資源オブジェクトに基づいている。各ユーザは、そのユーザのシステム内でのケイパビリティに基づいて、個々の資源オブジェクトにアクセスする権限を与えられる。AS/400システムは、ユーザ・プロフィール、オブジェクト権限およびシステム値をマシン自体のアーキテクチャ内で保持することによって、セキュリティを維持する。上記と同様に、このシステムは、単一のホストによって制御される資源オブジェクトへのアクセスを制御する点では非常に効率的であるが、複数のホストを含む分散データ処理システム内にある資源オブジェクトへのアクセスは制御できない。すなわち、あるホストによって制御されている資源オブジェクトへのアクセス権を、第2のホストに登録されたユーザが得ることはできない。

【0005】アクセス制御システムのもう1つの例が、製品DB2（データベース2）である。この製品は、より柔軟なアクセス制御が可能であり、細分的なまたはバンドルされたアクセス制御権限を提供する。たとえば、DB2システムは、システム管理用またはデータベース操作の特別な権限を利用できる。さらに、アクセス特権を指定された権限または役割にまとめて、ユーザが、そのユーザ個人の識別ではなく、そのユーザの肩書または権限レベルに基づいて、特定の資源オブジェクトにアクセスできるようにすることができる。しかし、上記と同様に、DB2システムは、非DB2アプリケーションとアクセス制御情報を交換する能力をもたない。

【0006】

【発明が解決しようとする課題】したがって、分散デー

タ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が必要であることは明白である。

【0007】したがって、本発明の1つの目的は、改良されたデータ処理システムを提供することである。

【0008】本発明の他の目的は、分散データ処理システム内の複数の資源オブジェクトに対するアクセス制御を実現する、改良された方法を提供することである。

【0009】本発明の他の目的は、分散データ処理システム内の複数の資源オブジェクトに対するアクセス制御を実現し、分散データ処理システム全体を通じて、高速かつ効率的なアクセス制御情報の交換を可能にする、改良された方法を提供することである。

【0010】

【課題を解決するための手段】前述の目的は、以下に述べるようにして達成される。本発明の方法を利用して、複数の資源マネージャを有する分散データ処理システム内で複数の資源オブジェクトに対するユーザ・アクセスの制御を実現することができる。参照モニタ・サービスを確立し、複数のアクセス制御プロフィールをそこに記憶する。その後、ある資源マネージャによって制御される特定の資源オブジェクトへのアクセスの試みに応答して、選択されたアクセス制御プロフィールが、参照モニタ・サービスとその資源マネージャの間で交換される。その後、資源マネージャは、交換されたアクセス制御プロフィールを用いて、その資源オブジェクトに対するアクセスを制御することができる。本発明の好ましい実施例では、それぞれのアクセス制御プロフィールは、選択されたユーザ、選択された資源オブジェクト、選択されたユーザ・グループ、選択された資源オブジェクト・グループ、あるいは所定の1組の資源オブジェクトと、それぞれが前記所定の1組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストに関するアクセス制御情報を含む。

【0011】

【実施例】図面、特に図1を参照すると、本発明の方法を実施するために利用される分散データ処理システム8が示されている。図からわかるように、分散データ処理システム8は、ローカル・エリア・ネットワーク（LAN）10と32など複数のネットワークを含み、それぞれのネットワークは、それぞれ複数の個々のコンピュータ12および30を含むことが好ましい。もちろん、前述のネットワークのそれぞれに、ホスト・プロセッサに結合された複数の対話型ワーク・ステーション（IWS）を使用してもよいことは、当業者には理解されよう。

【0012】このようなデータ処理システムでは一般的なことであるが、それぞれのコンピュータは、記憶装置

14またはプリンタ/出力装置16あるいはその両方に結合することができる。本発明の方法によれば、1つまたは複数の前述の記憶装置14を利用して、分散データ処理システム8内の任意のユーザによって定期的にアクセスされるアプリケーションまたは資源オブジェクトを記憶することができる。記憶装置14に記憶された前述のアプリケーションまたは資源オブジェクトはそれぞれ、当技術分野で周知の方式で資源マネージャに関連づけられる。資源マネージャは、それに関連づけられたすべての資源オブジェクトを維持し更新する責任を負う。

【0013】図1によれば、分散データ処理システム8は、メイン・フレーム・コンピュータ18など、複数のメイン・フレーム・コンピュータをも含む。これらのメイン・フレーム・コンピュータは、通信リンク22によってLAN10に結合することが好ましい。メイン・フレーム・コンピュータ18は、LAN10用の遠隔記憶装置として働く記憶装置20にも結合される。同様に、LAN10は、通信リンク24を介し、サブシステム制御装置/通信制御装置26および通信リンク34を通じて、ゲートウェイ・サーバ28に結合される。ゲートウェイ・サーバ28は、LAN32をLAN10にリンクする働きをする、独立のコンピュータまたはIWSであることが好ましい。

【0014】LAN32およびLAN10に関して上述したように、資源オブジェクトは、記憶装置20内に記憶され、記憶されたその資源オブジェクト用の資源マネージャとしてのメイン・フレーム・コンピュータ18によって制御される。もちろん、メイン・フレーム・コンピュータ18は、地理的にLAN10から非常に遠く離れた所にあつてよく、同様に、LAN10も、LAN32から離れた所にあつてよいことが、当業者には理解されよう。すなわち、LAN32がカリフォルニアにあり、LAN10がテキサスにあり、メイン・フレーム・コンピュータ18がニューヨークにあつてもよい。

【0015】この形式の既知の従来技術のシステムでは、個々のコンピュータ30のユーザが、メイン・フレーム・コンピュータ18に関連する記憶装置20に記憶されたある資源オブジェクトにアクセスしたいと望む場合、コンピュータ30のユーザが、メイン・フレーム・コンピュータ18のセキュリティ・システムに登録される必要がある。これは、コンピュータ30のユーザが、所望の資源オブジェクトへのアクセスを得るのに適当なパスワードを提示するために必要である。もちろん、この技法が、図1に示したデータ処理システムなどの分散データ処理システムではうまく働かないことは、当業者には理解されよう。

【0016】次に図2を参照すると、本発明の方法と共に利用されるアクセス制御システムが、ブロック図で示されている。図によれば、LAN10および32は破線で示されており、メイン・フレーム・コンピュータ18

も同様である。いずれの場合も、資源オブジェクト42、48、54が、図1の分散データ処理システム8のそれぞれの部分と関連づけて示されている。もちろん、図の各オブジェクトは、分散データ処理システム8のそれぞれの部分に関連する1つまたは複数の記憶装置に記憶される。図に示されるように、LAN10は、選択された資源オブジェクトを管理するために利用される1つまたは複数の個別のコンピュータである、資源マネージャ40を含む。LAN10の内部には、参照モニタ44も確立されている。参照モニタ44は、本発明の方法によれば、アクセス制御プロファイルを記憶するのに利用されるアプリケーションまたはサービスであり、アクセス制御プロファイルは、選択されたユーザ、選択された資源オブジェクト、選択されたユーザ・グループ、選択された資源オブジェクト・グループ、あるいは所定の1組の資源オブジェクトと、それぞれが前記所定の1組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストに関するアクセス制御情報を含む。

【0017】さらに図2を参照すると、LAN33の内部に、当技術分野で周知の方式で資源オブジェクト48へのアクセスを制御するために利用される、資源マネージャ46が示されている。同様に、参照モニタ50が、LAN32内に確立されている。前述したように、参照モニタ50を利用して、LAN32内の個々のユーザならびにLAN32内に記憶されている資源オブジェクトに関するアクセス制御プロファイルを記憶することが好ましい。

【0018】最後に、メイン・フレーム・コンピュータ18は、1つまたは複数の資源オブジェクト54と関連づけられた、資源マネージャ52を含むものとして図示されている。

【0019】本発明の重要な特徴によれば、資源オブジェクト42、48、54などの資源オブジェクトにアクセスを試みると、自動的に、1つまたは複数の参照モニタ・アプリケーションに対して、関連する資源マネージャが照会を行い、要求されたアクセスが許可されているか否かを判定する。本発明の図示の実施例によれば、データ処理システム8に必要な参照モニタ・アプリケーションは1つだけであるにもかかわらず、2つが図示されていることに留意されたい。本発明の方法によれば、各資源マネージャがすべて分散データ処理システム8内にある状態で、単一の参照モニタ・アプリケーション間の通信リンクが確立され(図1参照)、その結果、選択された資源オブジェクトへのアクセスを、その参照モニタ内のプロファイルに記憶されたアクセス制御情報に従って制御することができる。

【0020】このようにして、LAN32内のユーザは、図1に示した通信リンク(22、24、34)を介して、メイン・フレーム・コンピュータ18に関連する

資源オブジェクト54へのアクセスを要求できる。後でさらに詳しく説明するように、資源マネジャ52は、次に、参照モニタ44または参照モニタ50あるいはその両方に照会を行って、要求されたアクセスを許可するプロファイルが存在するか否かを決定する。存在する場合は、そのプロファイル情報が、適当な参照モニタと資源マネジャ52の間で交換され、資源オブジェクト54へのアクセスが許可される。

【0021】次に図3を参照すると、本発明の方法によるアクセス制御システムの確立を示す、高水準流れ図が示されている。図に示すように、ブロック60で処理が始まり、その後ブロック62に移って、あるオブジェクトまたはオブジェクト・グループ(42、48、54)用のアクセス制御プロファイルが、関連する資源マネジャ(40、46、52)によって定義される。その後、ブロック64で、そのプロファイルが参照モニタ・アプリケーション(44、50)に記憶される。次に、ブロック66で、アクセス制御プロファイルの確立を必要とするオブジェクトが他にもまだあるか否かを判定し、存在する場合には、ブロック62に戻って、それ以降繰り返して続行する。

【0022】アクセス制御プロファイルを必要とする資源オブジェクトが他にもない場合は、ブロック68に移って、関連する資源マネジャ(40、46、52)が、分散データ処理システム8内の1人または複数のユーザに対するアクセス制御プロファイルを確立する。その後、ブロック70で、このようにして作成されたアクセス制御プロファイルを、関連する参照モニタ・アプリケーション(44、50)に記憶する。次にブロック72で、アクセス制御プロファイルの作成を必要とするユーザがデータ処理システム8内に他にまだいるか否かを判定する。まだいる場合は、上述と同様に、ブロック68に戻って、追加のプロファイルを定義する。アクセス制御プロファイルを必要とするユーザが他にもない場合は、ブロック74で、処理は終了する。もちろん、このようにして、1つの資源オブジェクト、資源オブジェクト・グループ、1人のユーザ、ユーザ・グループ、あるいは所定の1組の資源オブジェクトと選択されたユーザ・グループに関するアクセス制御情報を含む様々なアクセス制御プロファイルを作成できることが、当業者には理解されよう。

【0023】最後に、図4を参照すると、本発明の方法による資源オブジェクトへのアクセスを示す、高水準の流れ図が示されている。図に示すように、ブロック80で処理が始まり、その後ブロック82に移って、資源マネジャ(40、46、52)が、その資源マネジャの範囲内にある資源オブジェクト(42、48、54)に対するアクセス要求を受け取る。次に、ブロック84に移って、最も近くにある参照モニタ・アプリケーション(44、50)の照会を行って、問題の資源オブジェ

クトまたはユーザに対するアクセス制御プロファイルが存在するか否かを判定する。

【0024】次にブロック86で、適当なアクセス制御プロファイルが局所で定義されているか否かを判定し、定義されている場合には、ブロック88で、その特定の資源オブジェクトへのアクセスが許可されているか否かを判定する。この判定は、当業者には理解されるように、定義されたアクセス制御プロファイルを、問題の資源オブジェクトおよびユーザのパラメータと比較するだけのことである。その後、ブロック88での判定で許可される場合、ブロック90で、資源オブジェクトへのアクセスが提供され、その後ブロック92で処理が終了する。

【0025】ブロック86に戻って、アクセス制御プロファイルが局所で定義されていない場合は、ブロック94で、適当なアクセス制御プロファイルがシステム内のどこかで定義されているか否かを判定する。定義されている場合は、ブロック96でそのプロファイルを検索し、次にブロック88に戻って、選択された資源オブジェクトへのアクセスが許可されているか否かを判定する。その後、アクセスが許可される場合には、ブロック90に移って、資源オブジェクトへのアクセスが行われ、その後処理が終了する。

【0026】必要とされるアクセス制御プロファイルが、分散データ処理システム8(図1参照)内のどこでも定義されていないか、または所望の資源オブジェクトへのアクセスが許可されていないとブロック88で判定された場合は、ブロック98で、要求元へ適当なメッセージを送って、要求された資源オブジェクトへのアクセスを拒否する。

【0027】以上の説明を参照すれば、それぞれが資源オブジェクトまたはユーザに関する1つまたは複数のアクセス制御プロファイルを含む、分散データ処理システム内の1つまたは複数の参照モニタ・アプリケーションを利用することによって、分散データ処理システム8内のそれぞれのユーザが、システム内のすべての地点にあるそれぞれの資源マネジャに登録する必要なしに、分散データ処理システムの様々な部分にある複数の資源オブジェクトへのアクセスを制御できることが、当業者には理解されよう。システム全体を通じたアクセス制御情報を含むアクセス制御プロファイルを、高速かつ効率的に交換できるようにすることによって、必要なアクセス制御の決定が限られた数の位置で行われ、処理の効率が大きく改善される。

【0028】

【発明の効果】分散データ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が実現された。

【図面の簡単な説明】

【図1】本発明の方法を実施するために利用できる分散データ処理システムを示す図である。

【図2】本発明の方法と共に利用されるアクセス制御システムのブロック図である。

【図3】本発明の方法によるアクセス制御システムの確立を示す、高水準の流れ図である。

【図4】本発明の方法による資源オブジェクトへのアクセスを示す、高水準の流れ図である。

【符号の説明】

8 分散データ処理システム

10 ローカル・エリア・ネットワーク (LAN)

12 コンピュータ

14 記憶装置

16 プリンタ/出力装置

18 メイン・フレーム・コンピュータ

20 記憶装置

22 通信リンク

24 通信リンク

26 サブシステム制御装置/通信制御装置

28 ゲートウェイ・サーバ

30 コンピュータ

32 ローカル・エリア・ネットワーク (LAN)

34 通信リンク

40 資源マネージャ

10 42 資源オブジェクト

44 参照モニタ

46 参照モニタ

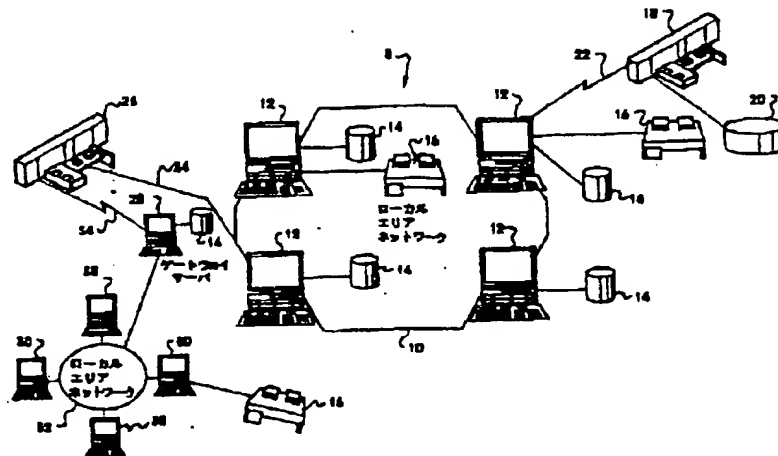
48 資源オブジェクト

50 資源マネージャ

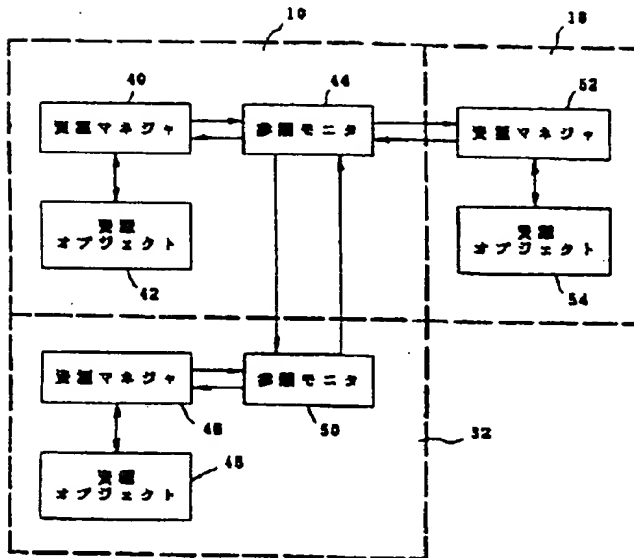
52 資源オブジェクト

54 参照モニタ

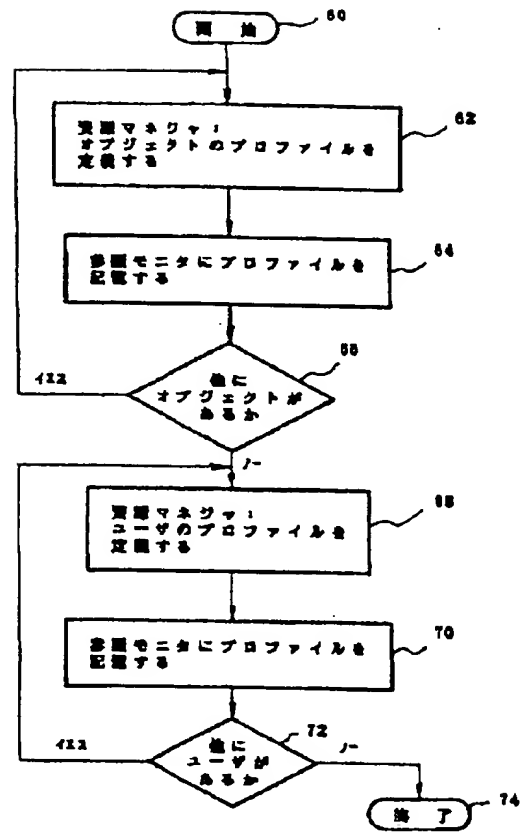
【図1】



【図2】



【図3】



【図4】

